

EchoLife GPON Terminal HG8245T/HG8247T User Manual



EchoLife GPON Terminal HG8245T/HG8247T
V200R006C00S102

User Manual

Huawei Technologies Co., Ltd. provides customers with comprehensive technical support and service. Please feel free to contact our local office or company headquarters.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: <http://www.huawei.com>

Email: support@huawei.com

Copyright © Huawei Technologies Co., Ltd. 2013. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions



and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

NO WARRANTY

THE CONTENTS OF THIS MANUAL ARE PROVIDED "AS IS". EXCEPT AS REQUIRED BY APPLICABLE LAWS, NO WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, ARE MADE IN RELATION TO THE ACCURACY, RELIABILITY OR CONTENTS OF THIS MANUAL.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO CASE SHALL HUAWEI TECHNOLOGIES CO., LTD. BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT, OR CONSEQUENTIAL DAMAGES, OR LOST PROFITS, BUSINESS, REVENUE, DATA, GOODWILL OR ANTICIPATED SAVINGS.

Import and Export Regulations

Customers shall comply with all applicable export or import laws and regulations and will obtain all necessary governmental permits and licenses in order to export, re-export or import the product mentioned in this manual including the software and technical data therein.

Privacy Policy

Please refer to our privacy policy on our websites for the information about how we protect your personal information.

Contents

1 Safety Precautions	1
2 System Overview	3
2.1 Product Introduction	3
2.1.1 HG8245T	4
2.1.2 HG8247T	9
2.2 Technical Specifications	14
2.2.1 Physical Specifications	14
2.2.2 Protocols and Standards	15
2.3 Typical Network Applications	15
3 Hardware Installation	17
3.1 Installing the Terminal	17
3.1.1 Placing the Terminal on the Desk	17
3.1.2 Mounting the Terminal onto the Wall	18
3.2 Connecting Cables	18
4 Logging in to the Web Configuration Window	21
5 Web Page Reference	24
5.1 Status	25
5.1.1 WAN Information	25
5.1.2 VoIP Information	25
5.1.3 WLAN Information	26
5.1.4 Eth Port Information	26
5.1.5 DHCP Server Information	27
5.1.6 Optic Information	27
5.1.7 Battery Information	28
5.1.8 User Device Information	28
5.2 WAN	29
5.3 LAN	29
5.3.1 LAN Host Configuration	29
5.3.2 DHCP Server Configuration	30
5.4 WLAN	32
5.4.1 WLAN Configuration	32
5.5 Security	35
5.5.1 IP Filter Configuration	35

5.5.2 MAC Filter Configuration	36
5.5.3 URL Filter Configuration	37
5.5.4 DoS Configuration	38
5.6 Forward Rules	39
5.6.1 DMZ Configuration	39
5.6.2 PortMapping Configuration	41
5.6.3 PortTrigger Configuration	42
5.7 Network Applications	43
5.7.1 USB	43
5.7.2 ALG Configuration	45
5.7.3 UPnP Configuration	45
5.7.4 ARP Configuration	46
5.7.5 DDNS Configuration	46
5.7.6 IGMP Configuration	47
5.7.7 QoS Configuration	48
5.7.8 DNS Configuration	48
5.8 System Tools	49
5.8.1 Reboot	49
5.8.2 Configuration File	49
5.8.3 Restore Default Configuration	50
5.8.4 Maintenance	51
5.8.5 Voice Remote Mirroring	51
5.8.6 Log	52
5.8.7 ONT Authentication	52
5.8.8 Advanced Power Management	53
5.8.9 Modify Login Password	54
6 FAQs	55
7 Appendix	56
7.1 Indicators	56
7.2 Acronyms and Abbreviations	56

1 Safety Precautions

To ensure normal running of the device, read the safety precautions carefully before operating the device, and comply with the precautions when performing the operations.

Basic Requirements

- Keep the device dry during storage, transportation, and running of the device.
- Prevent the device from colliding with other objects during storage, transportation, and running of the device.
- Install the device in strict compliance with the vendor requirements.
- Do not uninstall the device without permission. Contact the specified service center when a fault occurs on the device.
- No enterprise or personnel should modify the structure, security design, or performance design of the device without authorization.
- Abide by local laws and regulations and respect the legal rights of others when using the device.

Environment Requirements

- Install the device in a well-ventilated place that is not directly exposed to sunlight.
- Keep the device clean.
- Keep the device away from water sources or wet places.
- Do not place any objects on the device. This is to protect the device from damages, such as overheat or distortion, which can be caused by such objects.
- Leave a space of at least 10 cm around the device for heat dissipation.
- Keep the device away from heat sources or fire sources, such as electrical heaters and candles.
- Keep the device away from the electrical appliances with strong magnetic fields or strong electric fields, such as microwave ovens, refrigerators, and mobile phones.

Instructions for Use

- Use the accessories delivered with the device, or use those recommended by the vendor, such as the power adapter and battery.
- The power supply voltage of the device must meet the requirements on the input voltage of the device.

- Keep power plugs clean and dry to avoid electric shocks or any other hazards.
- Dry your hands before removing or inserting cables.
- Stop the device and switch off the power before removing or inserting cables.
- Switch off the power and remove all the cables, including the power cable, optical fibers, and network cables, from the device during periods of lightning activity.
- Switch off the power and remove the power plug if the device needs to be shut down for a long time.
- Protect the device from ingress of water or other liquids. If such an accident occurs, switch off the power immediately and remove all the cables, including the power cable, optical fibers, and network cables, from the device. Contact the specified service center in the case of a device failure.
- Do not stamp, pull, drag, or excessively bend the cables because they may get damaged. Damaged cables can cause a device failure.
- Do not use the cables that are damaged or have deteriorated.
- Do not look directly into the optical port on the device without eye protection. The laser emitted from the optical port can injure your eyes.
- In case of any abnormalities, such as smoke, abnormal sound, or odor from the device, immediately stop the device, switch off the power, and remove all cables, including the power cable, optical fibers, and network cables, from the device. Contact the specified service center in the case of a device failure.
- Prevent foreign objects such as metal objects from dropping into the device through the heat dissipation mesh.
- Protect the outer case of the device from scratches, because the paint that peels off in the scratched areas can cause device abnormalities. If the paint falls into the device it may cause short circuits. In addition, peeled-off paint can cause an allergic reaction to the human body.
- Ensure that the device is kept out of the reach of children. Guard against risks such as children playing with the device or swallowing small parts of the device.

Instructions for Cleaning

- Before cleaning the device, stop the device from running, switch off the power, and remove all cables, including the power cable, optical fibers, and network cables, from the device. When inserting and removing optical fibers, keep the optical fiber connectors clean.
- Do not use cleaning fluid or spray-on detergent to clean the outer case of the device. Use a soft cloth instead.

Instructions for Environment Protection

- Put the retired device and batteries at the specified recycle place.
- Abide by local laws and regulations to handle packaging materials, run-out batteries and retired devices.

2 System Overview

This topic provides the appearance and describes the typical network applications of the HG8245T/HG8247T.

2.1 Product Introduction

This topic provides the appearance and describes the ports and LEDs of the HG8245T/HG8247T.

2.2 Technical Specifications

This topic describes the technical specifications of the ONT, including its physical specifications and the standards and protocols which the ONT complies with.

2.3 Typical Network Applications

This topic describes the typical network applications of the HG8245T/HG8247T.

2.1 Product Introduction

This topic provides the appearance and describes the ports and LEDs of the HG8245T/HG8247T.

The HG8245T/HG8247T is an indoor optical network terminal (ONT) designed for home users and small office and home office (SOHO) users. Its upper shell adopts the natural heat dissipation material, and its optical port adopts the dust-proof design with a rubber plug. The HG8245T/HG8247T is eye-pleasing and energy-efficient. It can be deployed on a workbench or mounted on a wall, meeting users' deployment requirements in different scenarios.



NOTICE

The series ONTs are used indoors only. Do not install them outdoors or in outdoor cabinets.

By using the gigabit-capable passive optical network (GPON) technology, the HG8245T/HG8247T provides a high-speed data channel through a single optical fiber with an upstream rate of 1.244 Gbit/s and a downstream rate of 2.488 Gbit/s. In this way, you can enjoy quality high-speed data service, voice service, and video service. In addition, the

HG8245T and HG8247T provide reliable wireless access service and convenient storage and file sharing services within a home network.

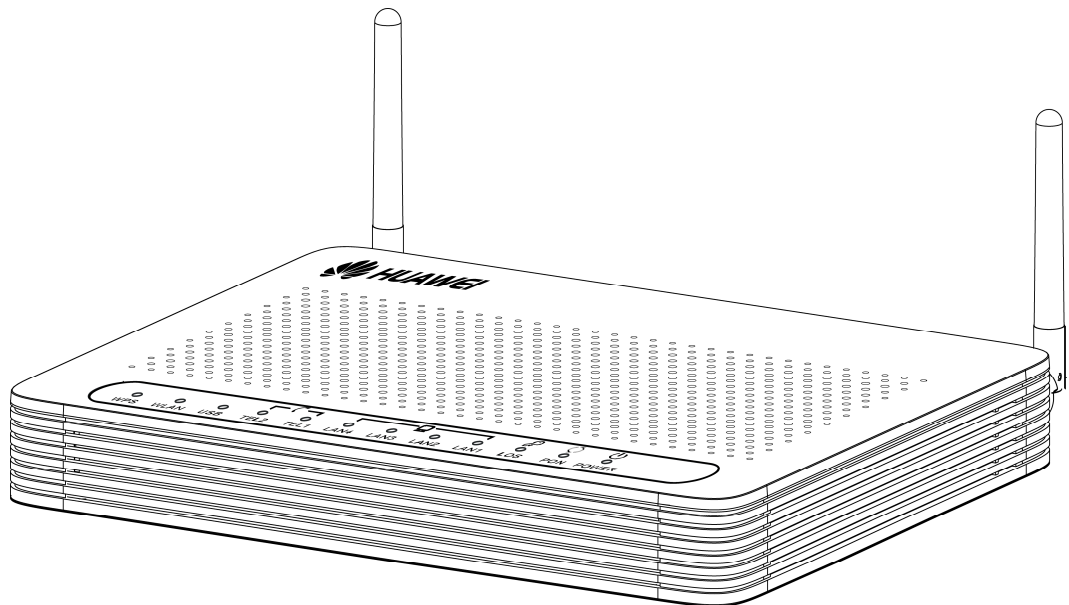
As an ONT, the HG8245T/HG8247T provides convenient and efficient remote management functions. The HG8245T/HG8247T supports ONT Management and Control Interface (OMCI) protocol and TR-069 server and manages all home terminals in a unified manner, thus implementing remote fault diagnosis, service provisioning, and performance statistics measurement.

2.1.1 HG8245T

Introduced the appearance, interfaces and LEDs of the HG8245T.

Appearance

Figure 2-1 Appearance of the HG8245T



Ports

[Figure 2-2](#) and [Figure 2-3](#) show the ports on the rear panel and side panel of the HG8245T respectively.

Figure 2-2 Ports on the rear panel of the HG8245T

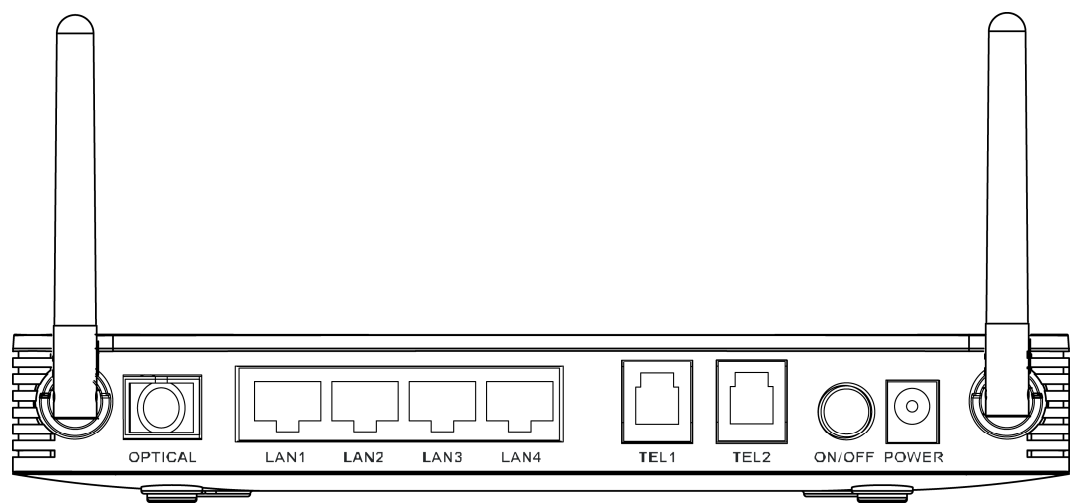


Table 2-1 Descriptions of the ports on the rear panel of the HG8245T

Port and Button	Function
OPTICAL	Indicates the optical port. The optical port is equipped with a rubber plug and is connected to an optical fiber for upstream transmission. The type of the optical connector connected to the OPTICAL port is SC/APC.
LAN1-LAN4	Indicate auto-sensing 10/100/1000M Base-T Ethernet ports (RJ-45), used for connecting to PCs or IP STBs.
TEL1-TEL2	Indicate VoIP telephone ports (RJ-11), used for connecting to the ports on telephone sets.
ON/OFF	Indicates the power-on/power-off button, used for powering on or powering off the device.
POWER	Indicates the power port, used for connecting to the power adapter or backup battery.

Figure 2-3 Ports on the side panel of the HG8245T

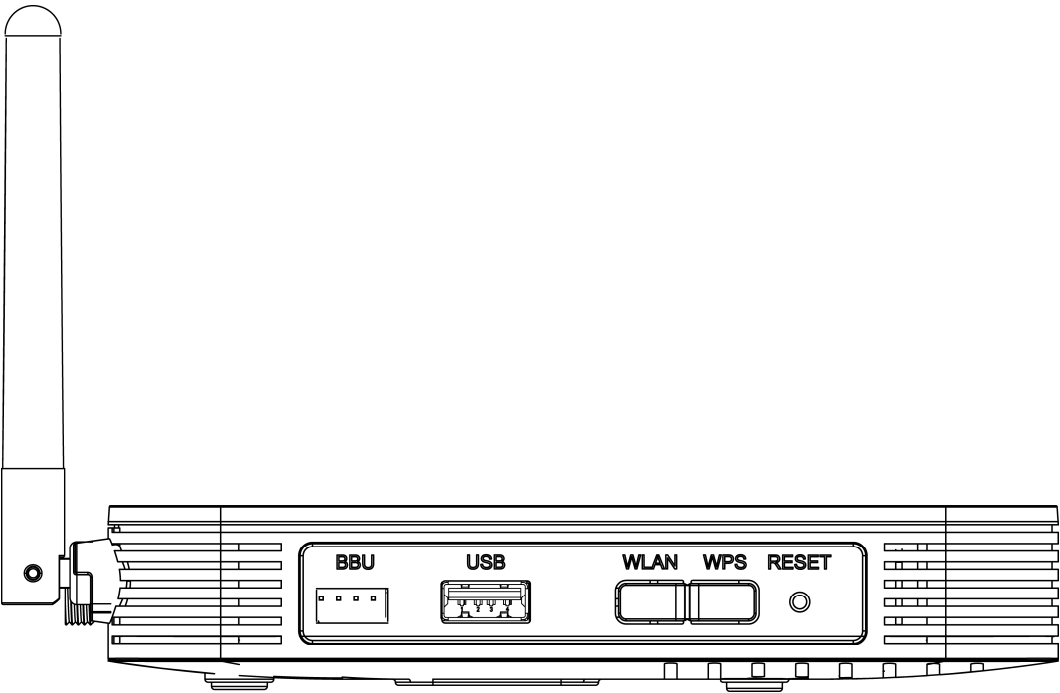


Table 2-2 Descriptions of the ports on the side panel of the HG8245T

Port and Button	Function
BBU	Indicates the external backup battery monitoring port, used for connecting to the backup battery for monitoring the battery.
USB	Indicates the USB host port, used for connecting to a USB storage device.
WLAN	Indicates the WLAN button, used for enabling or disabling the WLAN function.
WPS	Indicates the WLAN data encryption switch.
RESET	Indicates the reset button. Press the button for a short time to reset the device; press the button for a long time (longer than 10s) to restore the device to the default settings and reset the device.

LEDs

Figure 2-4 LEDs on the HG8245T

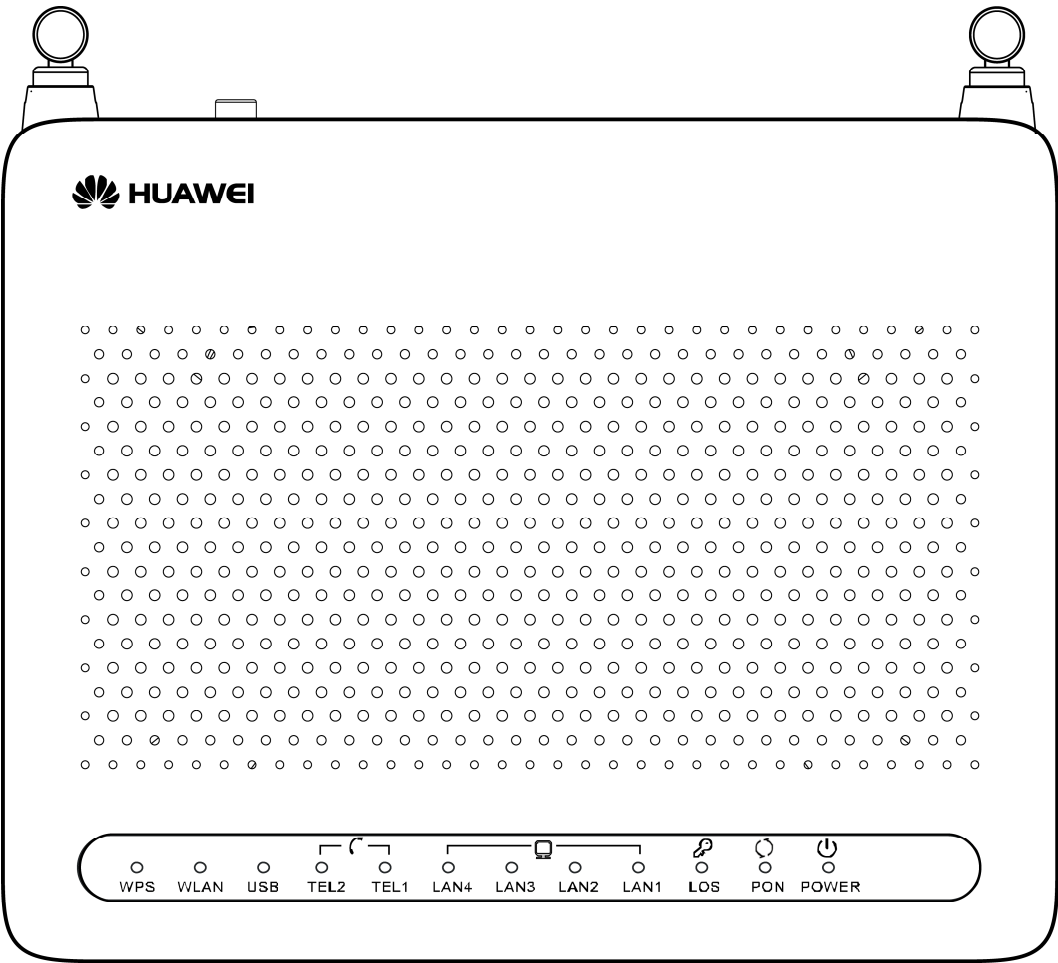


Table 2-3 Indications of the LEDs on the HG8245T

Silk Screen	Name	Status	Indication
POWER	Power supply LED	Green: always on	The device is powered on.
		Orange: always on	The device is powered by the backup battery.
		Off	The power supply is cut off.
PON	Authentication LED	See Table 2-4 .	
LOS	Connection LED	See Table 2-4 .	
LAN1-LAN4	Ethernet port LED	Always on	The Ethernet connection is in the normal state.

Silk Screen	Name	Status	Indication
		Blinks	Data is being transmitted on the Ethernet port.
		Off	The Ethernet connection is not set up.
TEL1-TEL2	Voice telephone port LED	Always on	The connection to the voice server is set up.
		Blinks quickly (twice per second)	The connection to the voice server is set up and the telephone is in the off-hook or ringing state.
		Blinks slowly (once two seconds)	The ONT is registering with the voice server.
		Off	The connection to the voice server is not set up.
USB	USB port LED	Always on	The USB port is connected and is working in the host mode, but no data is being transmitted.
		Blinks quickly (twice per second)	Data is being transmitted on the USB port.
		Off	The system is not powered on or the USB port is not connected.
WLAN	WLAN port LED	Always on	The WLAN function is enabled.
		Blinks	Data is being transmitted on the WLAN port.
		Off	The WLAN function is disabled.
WPS	WPS port LED	Always on	The WPS function is enabled.
		Blinks	A Wi-Fi terminal is accessing the system.
		Off	The WPS function is disabled.

Table 2-4 Indications of PON and LOS LEDs

No.	LED Status		Indication
	PON	LOS	
1	Off	Off	The ONT is disabled by the OLT.
2	Blinks quickly (twice per	Off	The ONT is attempting to set up a connection to the OLT.

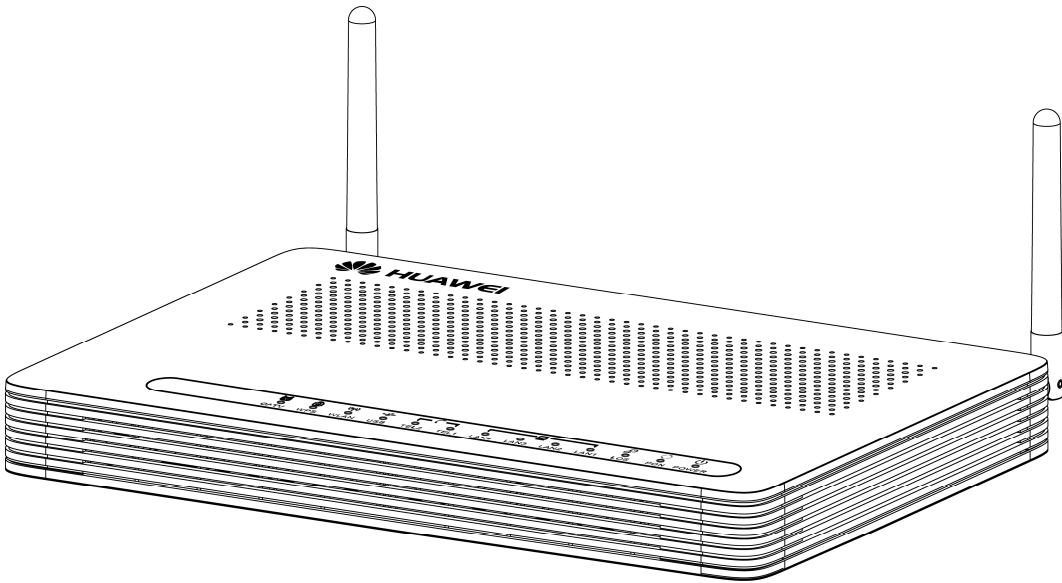
No.	LED Status		Indication
	PON	LOS	
	second)		
3	Always on	Off	The connection between the ONT and the OLT is set up.
4	Off	Blinks slowly (once two seconds)	The Rx optical power of the ONT is lower than the optical receiver sensitivity.
5	Blinks quickly (twice per second)	Blinks quickly (twice per second)	The OLT detects that the ONT is a rogue ONT.

2.1.2 HG8247T

Introduced the appearance, interfaces and LEDs of the HG8247T.

Appearance

Figure 2-5 Appearance of the HG8247T



Ports

Figure 2-6 and Figure 2-7 show the ports on the rear panel and side panel of the HG8247T respectively.

Figure 2-6 Ports on the rear panel of the HG8247T

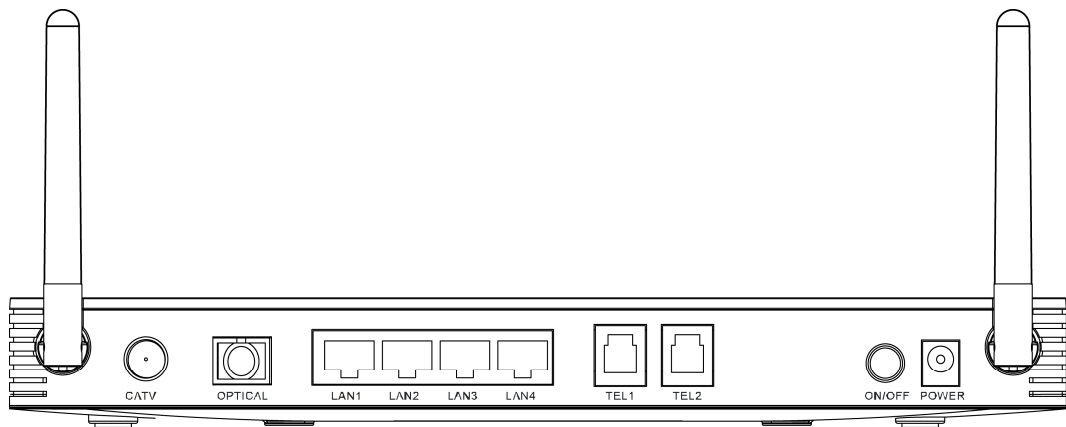


Table 2-5 Descriptions of the ports on the rear panel of the HG8247T

Port and Button	Function
CATV	Indicates an RF port, used to connect to a TV set.
OPTICAL	Indicates the optical port. The optical port is equipped with a rubber plug and is connected to an optical fiber for upstream transmission. The type of the optical connector connected to the OPTICAL port is SC/APC.
LAN1-LAN4	Indicate auto-sensing 10/100/1000M Base-T Ethernet ports (RJ-45), used for connecting to PCs or IP STBs.
TEL1-TEL2	Indicate VoIP telephone ports (RJ-11), used for connecting to the ports on telephone sets.
ON/OFF	Indicates the power-on/power-off button, used for powering on or powering off the device.
POWER	Indicates the power port, used for connecting to the power adapter or backup battery.

Figure 2-7 Ports on the side panel of the HG8247T

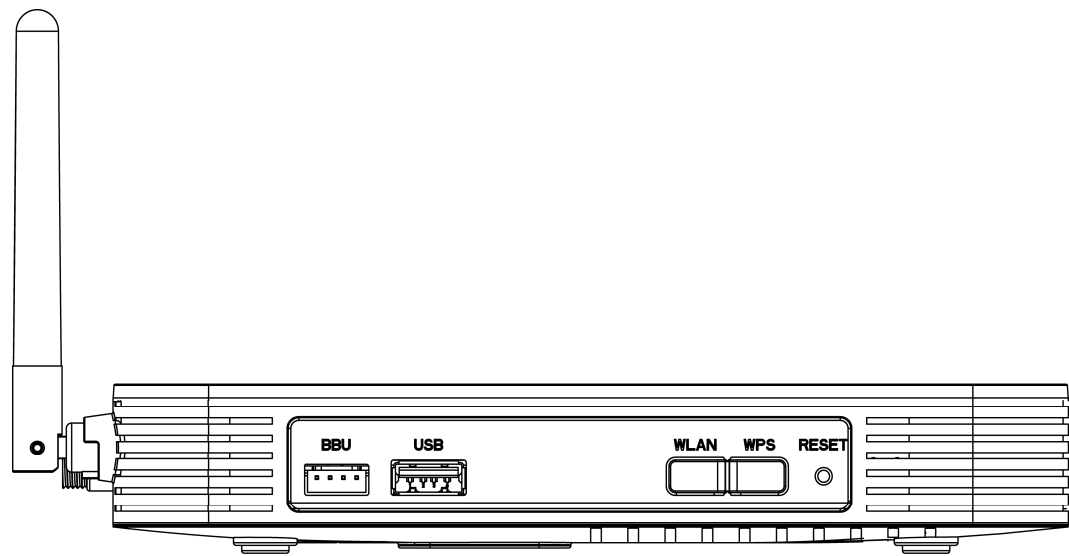


Table 2-6 Descriptions of the ports on the side panel of the HG8247T

Port and Button	Function
BBU	Indicates the external backup battery monitoring port, used for connecting to the backup battery for monitoring the battery.
USB	Indicates the USB host port, used for connecting to a USB storage device.
WLAN	Indicates the WLAN button, used for enabling or disabling the WLAN function.
WPS	Indicates the WLAN data encryption switch.
RESET	Indicates the reset button. Press the button for a short time to reset the device; press the button for a long time (longer than 10s) to restore the device to the default settings and reset the device.

LEDs

Figure 2-8 LEDs on the HG8247T

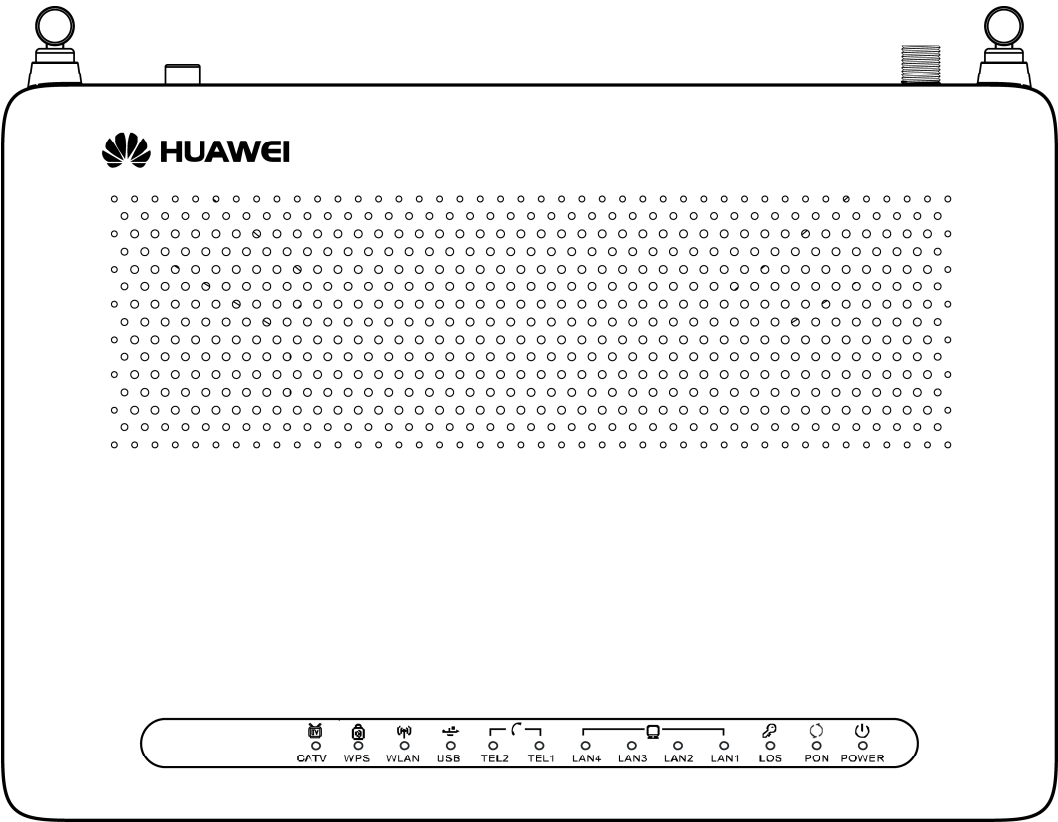


Table 2-7 Indications of the LEDs on the HG8247T

Silk Screen	Name	Status	Indication
POWER	Power supply LED	Green: always on	The device is powered on.
		Orange: always on	The device is powered by the backup battery.
		Off	The power supply is cut off.
PON	Authentication LED	See Table 2-8 .	
LOS	Connection LED	See Table 2-8 .	
LAN1-LAN4	Ethernet port LED	Always on	The Ethernet connection is in the normal state.
		Blinks	Data is being transmitted on the Ethernet port.
		Off	The Ethernet connection is not set up.

Silk Screen	Name	Status	Indication
TEL1-TEL2	Voice telephone port LED	Always on	The connection to the voice server is set up.
		Blinks quickly (twice per second)	The connection to the voice server is set up and the telephone is in the off-hook or ringing state.
		Blinks slowly (once two seconds)	The ONT is registering with the voice server.
		Off	The connection to the voice server is not set up.
USB	USB port LED	Always on	The USB port is connected and is working in the host mode, but no data is being transmitted.
		Blinks quickly (twice per second)	Data is being transmitted on the USB port.
		Off	The system is not powered on or the USB port is not connected.
WLAN	WLAN port LED	Always on	The WLAN function is enabled.
		Blinks	Data is being transmitted on the WLAN port.
		Off	The WLAN function is disabled.
WPS	WPS port LED	Always on	The WPS function is enabled.
		Blinks	A Wi-Fi terminal is accessing the system.
		Off	The WPS function is disabled.
CATV	CATV port LED	Always on	The CATV function is enabled and CATV signals are received.
		Off	The CATV function is disabled or CATV signals are not received.

Table 2-8 Indications of PON and LOS LEDs

No.	LED Status		Indication
	PON	LOS	
1	Off	Off	The ONT is disabled by the OLT.
2	Blinks quickly (twice per	Off	The ONT is attempting to set up a connection to the OLT.

No.	LED Status		Indication
	PON	LOS	
	second)		
3	Always on	Off	The connection between the ONT and the OLT is set up.
4	Off	Blinks slowly (once two seconds)	The Rx optical power of the ONT is lower than the optical receiver sensitivity.
5	Blinks quickly (twice per second)	Blinks quickly (twice per second)	The OLT detects that the ONT is a rogue ONT.

2.2 Technical Specifications

This topic describes the technical specifications of the ONT, including its physical specifications and the standards and protocols which the ONT complies with.

2.2.1 Physical Specifications

This topic describes the physical specifications of the ONT, including its dimensions, weight, voltage range, and environment parameters.

Table 2-9 lists the physical specifications of the HG8245T/HG8247T.

Table 2-9 Physical specifications

Item	HG8245T	HG8247T
Dimensions (length x width x depth)	195 mm x 174 mm x 34 mm	268 mm x 213 mm x 34 mm
Weight (including the power adapter)	About 550 g	About 800 g
Overall system power supply	11-14 V DC, 2 A	11-14 V DC, 2 A
Power adapter input range	100-240 V AC, 50-60 Hz	100-240 V AC, 50-60 Hz
Maximum power consumption	18W	20.5W
Temperature range	0°C to +40°C	0°C to +40°C
Humidity range	5%-95% (non-condensing)	5%-95% (non-condensing)

2.2.2 Protocols and Standards

This topic provides the protocols and standards which the ports of the ONT comply with.

- GPON: ITU-T G.984
- VoIP: H.248, SIP, G.711A/u, G.729a/b, and T.38
- Multicast: IGMPv2, IGMPv3, and IGMP snooping
- Routing: NAT, NAPT, and ALG
- Ethernet: IEEE 802.3ab
- USB: USB 1.1/USB 2.0
- Wi-Fi: IEEE 802.11n

2.3 Typical Network Applications

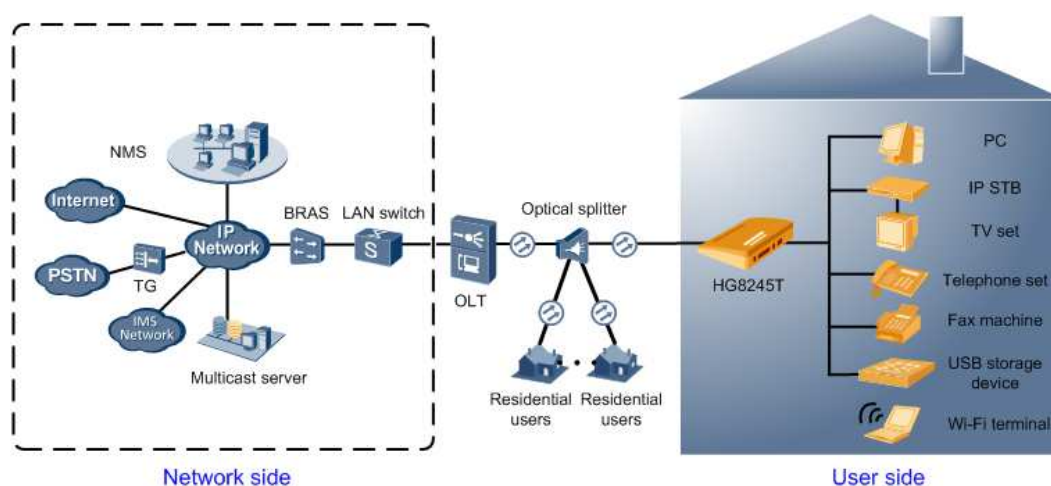
This topic describes the typical network applications of the HG8245T/HG8247T.

As a network terminal, the HG8245T/HG8247T is deployed at the GPON access layer and connects home users and SOHO users to the Internet through optical upstream ports. On the local area network (LAN) side, the HG8245T/HG8247T provides abundant hardware ports to meet various network requirements of home users and SOHO users.

Network Topology of the HG8245T

Figure 2-33 shows the position of the HG8245T in a network.

Figure 2-9 Network topology of the HG8245T



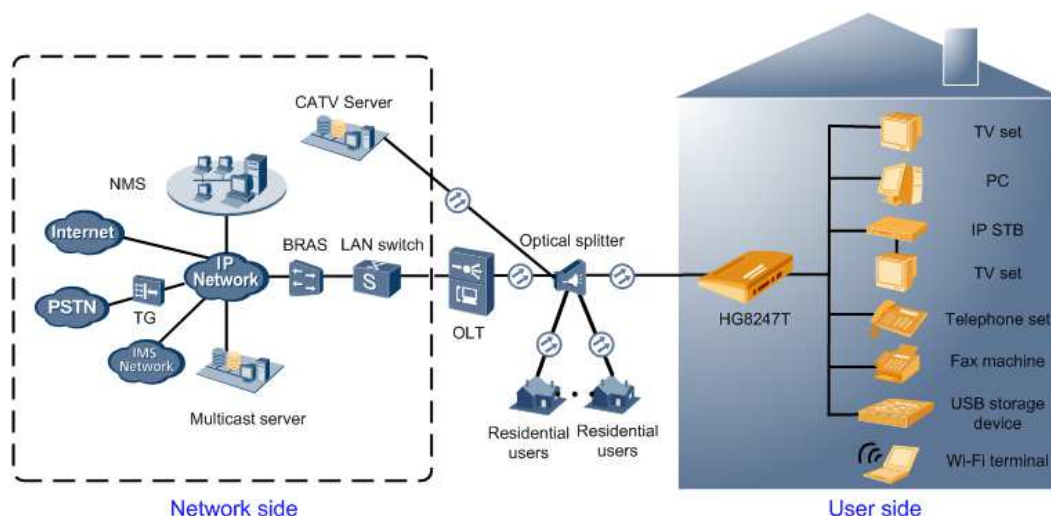
- In the upstream direction, the HG8245T is connected to the optical splitter and the network-side OLT through the PON port, namely the OPTICAL port, to provide integrated access services.
- In the downstream direction, the HG8245T is connected to various terminals through the following LAN-side ports to implement the triple play service:
 - Four 10/100/1000M Base-T Ethernet ports, which can be connected to terminals such as PCs, STBs, and video phones to provide the high-speed data and video services.

- Two TEL ports, which can be connected to telephone sets or fax machines to provide superior and cost-effective VoIP, FoIP, and MoIP services.
- Two Wi-Fi antennas, which can connect to Wi-Fi terminals wirelessly to provide a secure and reliable high-speed wireless network.
- One USB port, which can be connected to a USB storage device to provide convenient storage and file sharing services within a home network.

Network Topology of the HG8247T

Figure 2-10 shows the position of the HG8247T in a network.

Figure 2-10 Network topology of the HG8247T



- In the upstream direction, the HG8247T is connected to the optical splitter and the network-side OLT through the PON port, namely the OPTICAL port, to provide integrated access services.
- In the downstream direction, the HG8247T is connected to various terminals through the following LAN-side ports to implement the triple play service:
 - Four 10/100/1000M Base-T Ethernet ports, which can be connected to terminals such as PCs, STBs, and video phones to provide the high-speed data and video services.
 - Two TEL ports, which can be connected to telephone sets or fax machines to provide superior and cost-effective VoIP, FoIP, and MoIP services.
 - Two Wi-Fi antennas, which can connect to Wi-Fi terminals wirelessly to provide a secure and reliable high-speed wireless network.
 - One USB port, which can be connected to a USB storage device to provide convenient storage and file sharing services within a home network.
 - One CATV port, which can be connected to a TV set to provide high-quality CATV service transmission.

3 Hardware Installation



CAUTION

1. Do not install GPON terminals outdoors or on the outdoor cabinets.
2. GPON terminals can be mounted onto a wall or be placed on a workbench. Do not install GPON terminals in other modes, such as the ceiling.
3. The terminal cannot be connected to other devices such as GPON terminals, switch and router.

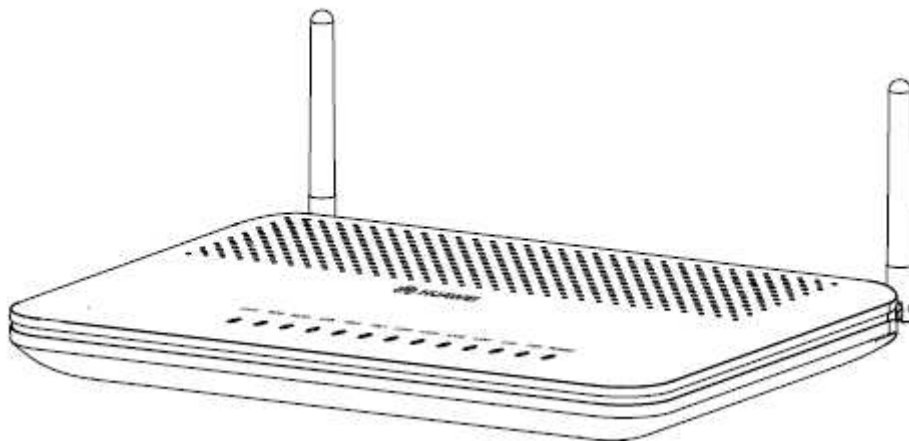
3.1 Installing the Terminal

There are two ways to install the terminal. One is placing the device on a stable and well-ventilated desk, and the other is mounting the device on to the wall.

3.1.1 Placing the Terminal on the Desk

The schematic diagram for placing the device on a desk horizontally are as follows:

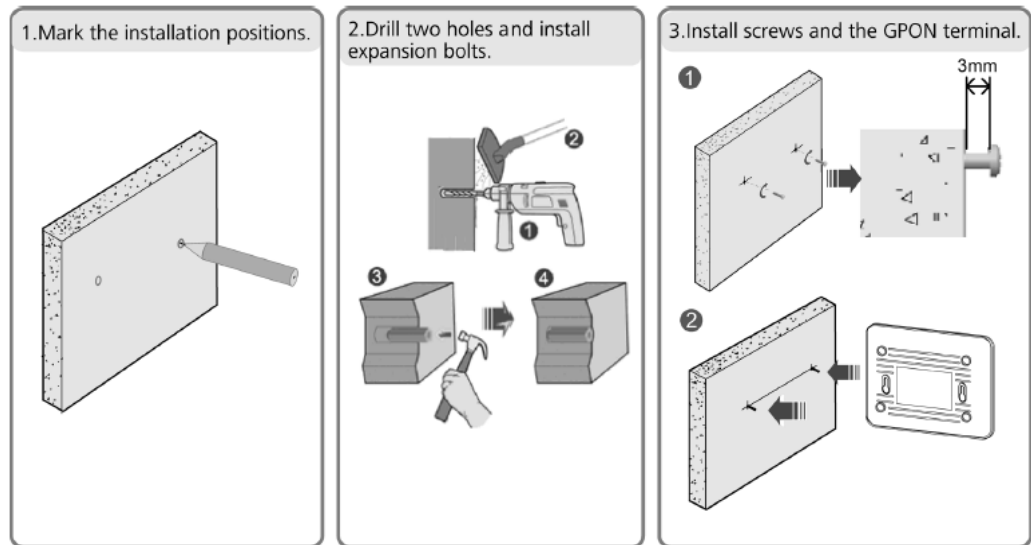
Figure 3-1 Placing the Device on the Desk



3.1.2 Mounting the Terminal onto the Wall

- Step 1** Mark the positions of two holes (with a spacing listed in the following table) used for mounting a GPON terminal.
- Step 2** Select a proper drill according to the outer diameter of the screws. Use a hammer drill to drill the marked positions on the wall. Then clean the wall and install two expansion bolts.
- Step 3** Use a screwdriver to fasten the screws into the expansion bolts, leaving the heads of the screws 3 mm over the wall. Then install the GPON terminal to the screws.

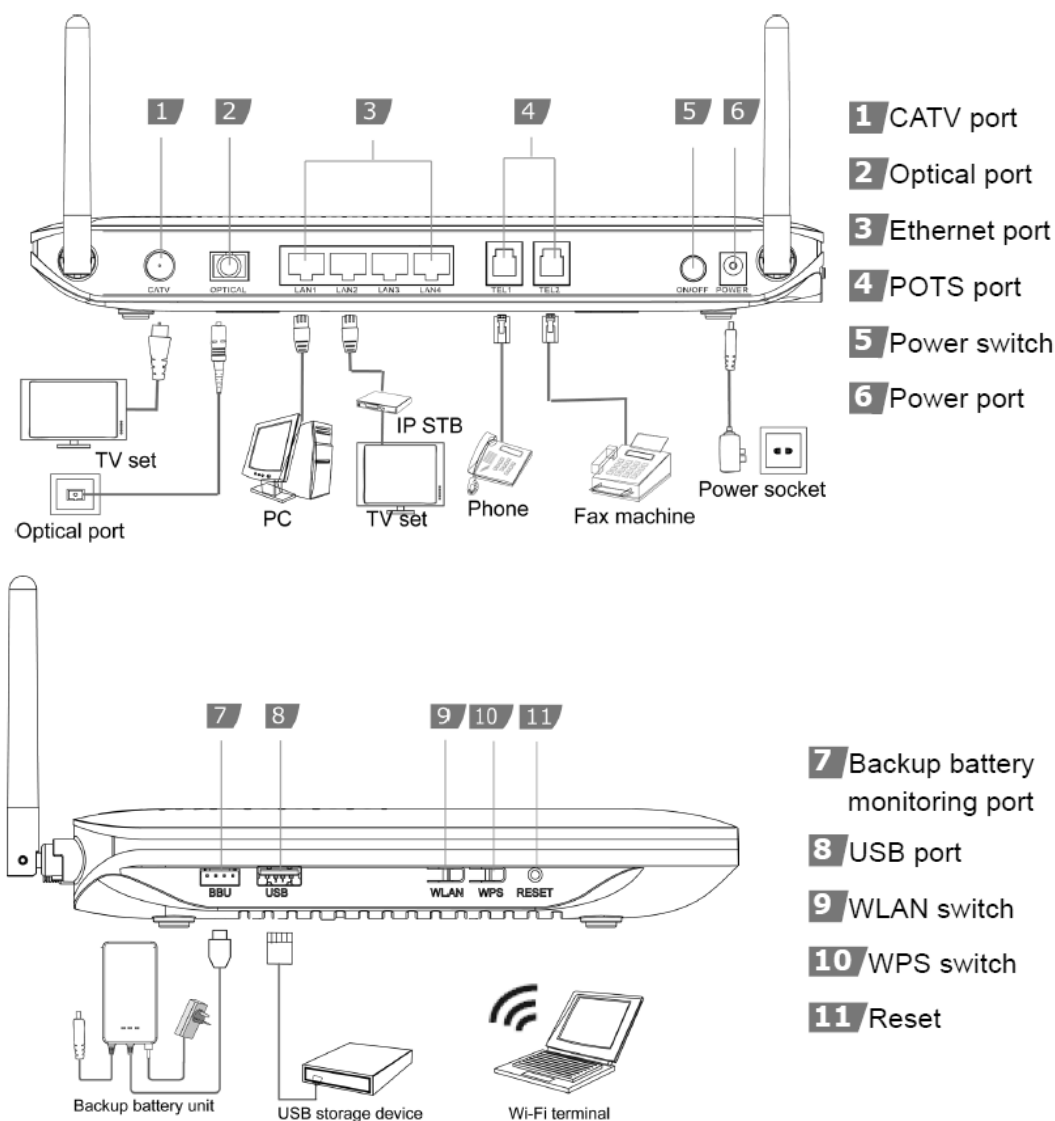
Figure 3-2 Mounting the Device onto the Wall



3.2 Connecting Cables

This document uses the HG8247T as an example to describe the connections. Ports on GPON terminals of other types may be different. Therefore, connect cables based on the ports that are actually supported by the device. If the external device is different from the device in the figure, refer to the description for connections of the external device.

Figure 3-3 Cable Connection



Step 1 Use an optical fiber to connect the **OPTICAL** port on the GPON terminal to the optical port in the wall.

NOTE

1. The optical connector connected to the **OPTICAL** port is an SC/APC connector, and the type of the optical connector connected to the optical port in the wall is determined by practical conditions.
2. To ensure normal use of fibers, make sure that the fiber bend radius is larger than 30 mm.

Step 2 Use a coaxial cable to connect the **CATV** port to a TV set or set top box (STB).

Step 3 Use a network cable to connect the **LAN** port to a PC or the Ethernet port on the IP STB.

Step 4 Use a phone line to connect the **TEL** port to a phone or fax machine.

Step 5 Use a power adapter to connect the **POWER** port to the power socket.

NOTE

The preceding figure connects the power adapter as an example. When connecting the backup battery unit, please see the usage guide to the backup battery for details.

Step 6 Use a USB data cable to connect the **USB** port to the USB storage device.

Step 7 Press the **ON/OFF** power switch.

Step 8 Press the **WLAN** switch to enable the Wi-Fi access function. By default, this function is enabled.

Step 9 Press the **WPS** switch to enable the WPS encryption function.



NOTE

Before enabling the WPS encryption function of a GPON terminal, ensure that the function is set in the system software in advance. After successful setting, press the WPS switch for the settings to take effect.

4 Logging in to the Web Configuration Window

This topic describes the data plan and procedure for logging in to the Web configuration interface.

Context

Before setting up the configuration environment, ensure that data information listed in [Table 4-1](#) is available.

Table 4-1 Data plan

Item	Description
User name and password	<p>Default settings:</p> <ul style="list-style-type: none">• Common user:<ul style="list-style-type: none">– User name: root– Password: admin <p>NOTE</p> <ul style="list-style-type: none">• After logging in to the web page, if you do not perform any operations within five minute, you will be locked out and return back to the login interface. Then, you can unlock the account by entering the login user name and password.• Three times the user name and password input error, the system is locked and unlocked automatically after one minute.• Modify the password through the Web.• Some pages can be hidden by the Service Provider. <p>NOTICE</p> <p>Change the initial password after logging in to the web page.</p>
LAN IP address and subnet mask	<p>Default settings:</p> <ul style="list-style-type: none">• IP address: 192.168.100.1• Subnet mask: 255.255.255.0

Item	Description
IP address and subnet mask of the PC	<p>Configure the IP address of the PC to be in the same subnet as the LAN IP address of the HG8245T/HG8247T.</p> <p>For example:</p> <ul style="list-style-type: none"> • IP address: 192.168.100.100 • Subnet mask: 255.255.255.0

Procedure

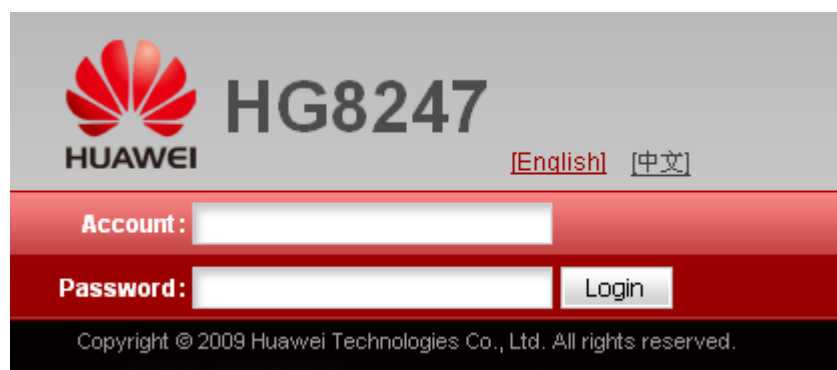
- Step 1** Use a network cable to connect the LAN port of the HG8245T/HG8247T to a PC.
- Step 2** Ensure that the Internet Explorer (IE) of the PC does not use the proxy server. The following section considers IE 6.0 as an example to describe how to check whether the IE uses the proxy server.
1. Start the IE, and choose **Tools > Internet Options** from the main menu of the IE window. Then, the **Internet Options** interface is displayed.
 2. In the **Internet Options** interface, click the **Connections** tab, and then click **LAN settings**.
 3. In the **Proxy server** area, ensure that the **Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections)** check box is not selected (that is, without the "✓" sign). If the check box is selected, deselect it, and then click **OK**.
- Step 3** Set the IP address and subnet mask of the PC. For details, see [Table 4-1](#).
- Step 4** Log in to the Web configuration interface.
1. Enter **http://192.168.100.1** in the address bar of IE (192.168.100.1 is the default IP address of the HG8245T/HG8247T), and then press **Enter** to display the login interface, as shown in [Figure 4-1](#).



NOTE

Web page login supports SSL3.0/TLS1.0/TLS1.1 protocols. If you use HTTPS to log in to the device, use TLS1.1 as recommended.

Figure 4-1 Login interface



2. In the login interface, enter the use name and password, and select your preferred language. For details about default settings of the user name and password, see [Table 4-1](#). After the password authentication is passed, the Web configuration interface is displayed.

----End

5 Web Page Reference

This topic describes the usage and meanings of the parameters on the Web Page.

Before configuring and viewing the parameters on the Web page, log in to the Web page. For details about how to log in to the Web page, see [Logging in to the Web Configuration Window](#).

5.1 Status

This topic describes how to query the information about the WAN interface, VoIP interface, and Wi-Fi port through the Web page.

5.2 WAN

This topic describes how to view the working mode of the WAN interfaces.

5.3 LAN

This topic describes how to set the working mode of the LAN port, the LAN host, and the DHCP server through the Web page.

5.4 WLAN

This topic describes how to perform basic and advanced configurations of the WLAN through the Web page.

5.5 Security

This topic describes how to configure the IP address filter, MAC address filter, DoS, and ONT access control through the Web page.

5.6 Forward Rules

This topic describes how to configure the DMZ, port mapping, and port trigger through the Web page.

5.7 Network Applications

This topic describes how to configure the USB, ALG, UPnP, and ARP through the Web page.

5.8 System Tools

This topic describes how to use the system tools on the Web page, including using the tools to restart the device, restore the default configuration, and conduct the test.

5.1 Status

This topic describes how to query the information about the WAN interface, VoIP interface, and Wi-Fi port through the Web page.

5.1.1 WAN Information

In the navigation tree on the left, choose **Status > WAN Information**. In the pane on the right, you can view the status of the WAN interface, mode of obtaining an IP address, IP address, and subnet mask, as shown in [Figure 5-1](#).

Figure 5-1 WAN Information

Status > WAN Information							
On this page, you can query the connection status and line status of the WAN interface.							
IPv4 Information							
WAN Name	Status	IP Acquisition Mode	IP Address	Subnet Mask	VLAN/Priority	MAC Address	Connect
1_INTERNET_R_VID_150	Connected	DHCP	192.168.11.52	--	150/0	70:7B:E8:76:5E:86	AlwaysOn
2_VOIP_R_VID_20	Disconnected	DHCP	--	--	20/1	70:7B:E8:76:5E:87	AlwaysOn
IPv6 Information							
WAN Name	Status	Prefix Acquisition Mode	Prefix	VLAN/Priority	MAC Address		
3_INTERNET_R_VID_108	Connected	PrefixDelegation		108/0	70:7B:E8:76:5E:88		
WAN Name	IP Acquisition Mode		IP Address		IP Address Status		
3_INTERNET_R_VID_108	LinkLocal		fe80::727b:e8ff:fe76:5e88		Preferred		

5.1.2 VoIP Information

In the navigation tree on the left, choose **Status > VoIP Information**. Then, in the pane on the right, you can query the information such as user status and call status. The SIP configuration page is slightly different from the H.248 configuration page, as shown in [Figure 5-2](#) and [Figure 5-3](#).

Figure 5-2 VoIP Information - SIP

Status > VoIP Information					
On this page, you can query the voice user list and status.					
Sequence	URI	User Name(Telephone Number)	Associated POTS	User Status	Call Status
1	--	88001234	1	Registering	Idle
2	--	88001235	2	Registering	Idle
To restart the VoIP service, click "Restart VoIP".					
<button>Restart VoIP</button>					

Figure 5-3 VoIP Information - H.248

Status > VoIP Information

On this page, you can query the voice user list and status.

Sequence	Line Name	Telephone Number	Associated POTS	User Status	Call Status	Interface Status
1	88001234	--	1	Registering	Idle	Closed
2	88001235	--	2	Registering	Idle	

To restart the VoIP service, click "Restart VoIP".

Restart VoIP

If the VoIP service needs to be restarted, click **Reset VoIP** in the pane on the right.

5.1.3 WLAN Information

In the navigation tree on the left, choose **Status > WLAN Information**. Then, in the pane on the right, you can query the information such as Wi-Fi port status, Wi-Fi packet statistics, and SSID, as shown in [Figure 5-4](#).

Figure 5-4 WLAN Information

Status > WLAN Information

On this page, you can query the WLAN status, WLAN statistics of packets and SSID Information.

WLAN Status

WLAN Enable:	Enable
WLAN Channel:	5

WLAN Statistics of Packets

SSID Index	SSID Name	Receive (Rx)				Transmit (Tx)			
		Bytes	Packets	Error	Discarded	Bytes	Packets	Error	Discarded
1	WirelessNet	131800	1087	0	0	471539	3565	0	0

SSID Information

SSID Index	SSID Name	Security Configuration	Authentication Mode	Encryption Mode
1	WirelessNet	Unconfigured	Open	None

- In the pane on the right, click **Enable** or **Disable** to enable or disable the Wi-Fi function.
- Click the link in blue to go to the corresponding configuration page.

5.1.4 Eth Port Information

In the navigation tree on the left, choose **Status > Eth Port Information**. In the pane on the right, you can view the duplex mode, speed, and status of the ETH port, as shown in [Figure 5-5](#).

Figure 5-5 Eth Port Information

Status > Eth Port Information							
On this page, you can query the information about user ports.							
Ethernet Port State							
Port	State			Receive (Rx)		Transmit (Tx)	
	Mode	Speed	Link	Bytes	Packets	Bytes	Packets
1	Full	1000M	Up	5171278	31089	7196899	26347
2	Half	10M	Down	0	0	0	0
3	Half	10M	Down	0	0	0	0
4	Half	10M	Down	0	0	0	0

5.1.5 DHCP Server Information

In the navigation tree on the left, choose **Status > DHCP Server Information**. In the pane on the right, you can view the basic information about the DHCP server, including the IP address assigned to the connected PC through DHCP, MAC address, and remaining lease time, as shown in [Figure 5-6](#).

Figure 5-6 DHCP Server Information

Status > DHCP Information				
On this page, you can query the basic information about the DHCP, including: host name, IP address, MAC address, remaining leased time, and device type.				
Host Name	IP Address	MAC Address	Remaining Leased Time	Device Type
iPhone	192.168.100.2	0c:77:1a:75:18:07	257925(s)	Computer
	192.168.100.3	5c:59:48:ec:bf:12	247533(s)	Computer

5.1.6 Optic Information

In the navigation tree on the left, choose **Status > Optic Information**. In the pane on the right, you can view the optical status, transmit optical power, receive optical power of the optical module, as shown in [Figure 5-7](#).

Figure 5-7 Optic Information

Status > Optical Information		
On this page, you can query the status of the optical transceiver.		
	Current value	Referenced value
Optical Status:	--	auto
Tx Optical Power:	--dBm	0.5 — 5dBm
Rx Optical Power:	--dBm	-27 — -8dBm
Working Voltage:	3330mV	3100—3500mV
Bias Current:	0mA	0—90mA
Working Temperature:	39°C	0—70°C
CATV Rx Power:	-30dBm	-8—2dBm
RF Output Power Level:	-30dBmv	17—25dBmv

5.1.7 Battery Information

In the navigation tree on the left, choose **Status > Battery Information**. In the pane on the right, you can view the connection status and available capacity of the external standby battery, as shown in [Figure 5-8](#).

Figure 5-8 Battery Information

Status > Battery Information	
On this page, you can look over the information about the power supply mode and the battery available capacity.	
Power Supply Mode:	AC Power
Battery Available Capacity:	0%

5.1.8 User Device Information

Click the **Status** tab and then choose **User Device Information** from the navigation tree. In the right pane, view the user device information, as shown in [Figure 5-9](#).

Figure 5-9 User Device Information

Status > User Device Information					
On this page, you can query the basic information about the user device, including: Host name, Device type, IP address, MAC address and Device status.					
Host Name	Device Type	IP Address	MAC Address	Device Status	Application
	Other	192.168.100.3	0c:77:1a:75:18:07	Offline	Detailed Info Communion Access Network Application
iPhone	Computer	192.168.100.2	0c:77:1a:75:18:07	Offline	Detailed Info Communion Access Network Application
myiPhone	Computer	192.168.100.3	60:fa:cd:30:f3:f2	Online	Detailed Info Communion Access Network Application
	Other	192.168.100.100	00:1b:21:c0:b9:81	Online	Detailed Info Communion Access Network Application

<< < 1/1 > >> Goto Page Go

5.2 WAN

This topic describes how to view WAN interface configuration through the Web page.

The WAN interface configuration is READ-ONLY. The settings are automatically configured by your service provider and cannot be changed.

5.3 LAN

This topic describes how to set the working mode of the LAN port, the LAN host, and the DHCP server through the Web page.

5.3.1 LAN Host Configuration

1. In the navigation tree on the left, choose **LAN > LAN Host Configuration**. In the pane on the right, set the management IP address and subnet mask of the LAN host, as shown in [Figure 5-10](#).

Figure 5-10 LAN Host Configuration

LAN > LAN Host Configuration	
On this page, you can configure LAN management IP addresses. After changing the LAN host IP address, ensure that the address pool configured in the DHCP server is the same subnet as the new LAN IP address. Otherwise, the DHCP server may not function properly.	
IP Address:	<input type="text" value="192.168.100.1"/> *
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	



NOTE

The IP address of the device connected to the LAN port must be in the same subnet as the management IP address. In this way, you can access an ONT through the Web page and perform query and management. You can manually set the IP address of the device connected to the LAN port to be on the same network segment as the management IP address, or start the DHCP server to set the IP address in the DHCP address pool to be on the same network segment as the management IP address. For details, see [5.2.2 DHCP Server Configuration](#).

- 2. Click **Apply** to apply the configuration.

5.3.2 DHCP Server Configuration

- 1. In the navigation tree on the left, choose **LAN > DHCP Server Configuration**. In the pane on the right, you can configure the LAN side DHCP address pool for the ONT that functions as a gateway. After the configuration, the PC connected to the LAN port can automatically obtain an IP address from the address pool, as shown in [Figure 5-11](#).

Figure 5-11 DHCP Server Configuration

LAN > DHCP Server Configuration

On this page, you can configure the DHCP Server parameters for the LAN side device including HGW, STB, Camera, Computer and Phone to obtain IP address.

Primary Address Pool

Enable primary DHCP server:

☒

Enable DHCP L2Relay:

☐

LAN Host IP Address:

192.168.100.1

Subnet Mask:

255.255.255.0

Start IP Address:

192.168.100.2

*(IP address must be in the same subnet with Lan Host)

End IP Address:

192.168.100.254

*

Leased Time:

3

day

Primary Address Pool Subsection

Device Type	Start IP Address	End IP Address
HGW:	192.168.100.10	192.168.100.29
STB:	192.168.100.80	192.168.100.89
Camera:	192.168.100.90	192.168.100.99
Computer:	192.168.100.100	192.168.100.200
Phone:	192.168.100.201	192.168.100.220

Secondary Address Pool

Enable secondary Server:

☒

IP Address:

192.168.2.1

*

Subnet Mask:

255.255.255.0

*

Start IP Address:

192.168.2.2

*

End IP Address:

192.168.2.254

*

Leased Time:

3

day

Option60:

MSFT 5.0

Apply

Cancel

- 2. Click **Apply** to apply the configuration.

[Table 5-1](#) describes the parameters related to the DHCP server.

Table 5-1 Parameters related to the DHCP server

Parameter	Description
Enable primary DHCP server	Indicates whether to enable the primary DHCP server. If the check box is selected, you can set the primary DHCP server.
Enable DHCP L2 Relay	<p>Indicates whether to enable the DHCP L2 Relay.</p> <p>The DHCP relay is a process in which cross-subnet forwarding of DHCP broadcast packets is implemented between the DHCP client and the DHCP server. In this manner, the DHCP clients in different physical subnets can obtain IP addresses which are dynamically allocated from the same DHCP server.</p> <ul style="list-style-type: none"> • If Mode of the WAN port is Route, the IP address of the ONT is obtained from upper-layer DHCP servers in different subnets and the user-side IP addresses are obtained from the DHCP address pool of the ONT. • If Mode of the WAN port is Bridge, the ONT functions as a bridge. Thus, the ONT does not have an IP address. The user-side IP addresses are obtained from upper-layer DHCP servers in different subnets.
Start IP Address	Indicates the start IP address in the IP address pool on the primary DHCP server. It must be in the same subnet as that of the IP address set in " LAN Host Configuration ". Otherwise, the DHCP server fails to work normally.
End IP Address	Indicates the end IP address in the IP address pool on the active DHCP server. It must be in the same subnet as that of the IP address set in " LAN Host Configuration ". Otherwise, the DHCP server fails to work.
Leased Time	Indicates the lease time of the IP address pool on the active DHCP server. Options: minute, hour, day, and week.
Enable secondary DHCP server	Indicates whether to enable the secondary DHCP server. If the check box is selected, you can set the secondary DHCP server.
IP Address	Indicates the IP address of the secondary DHCP server.
Subnet Mask	Indicates the subnet mask of the secondary

Parameter	Description
	DHCP server.
Start IP Address	Indicates the start IP address in the IP address pool on the secondary DHCP server.
End IP Address	Indicates the end IP address in the IP address pool on the secondary DHCP server.
Leased Time	Indicates the lease time of the IP address pool on the secondary DHCP server. Options: minute, hour, day, and week.
Option60	Indicates the option 60 field of the secondary DHCP server. A user-side DHCP client can obtain an IP address from the IP address pool on the secondary DHCP server only when the option 60 field carried by the user-side DHCP client is the same as this setting.

5.4 WLAN

This topic describes how to perform basic and advanced configurations of the WLAN through the Web page.

5.4.1 WLAN Configuration

1. In the navigation tree on the left, choose **WLAN > WLAN Configuration**. In the pane on the right, select the **Enable WLAN** option box. In the dialog box that is displayed, set the basic Wi-Fi parameters, including the SSID, authentication mode, and encryption mode, as shown in [Figure 5-12](#).

Figure 5-12 WI-FI Basic Configuration

WLAN > WLAN Configuration

On this page, you can set the WLAN parameters, including the WLAN switch, SSID configuration and channel selection.

☒ Enable WLAN

Basic Configuration New Delete

	SSID Index	SSID Name	SSID State	Associated Device Number	Broadcast SSID	Security Configuration
<input type="checkbox"/>	1	WirelessNet	Enable	32	Enable	Unconfigured

SSID Configuration in Detail

SSID Name: *

Enable SSID: ☒

Associated Device Number: *

Broadcast SSID: ☒

WMM Enable: ☒

Authentication Mode:

Encryption Mode:

Apply Cancel

Advance Configuration

Transmitting Power:

Regulatory Domain:

Channel:

Channel Width:

Mode:

DTIM Period: (1-255, default: 1)

Beacon Period: ms (20-1000ms, default: 100)

RTS Threshold: bytes (1-2346 bytes, default: 2346)

Frag Threshold: bytes (256-2346 bytes, default: 2346)

Apply Cancel

2. Click **Apply** to apply the configuration.

Table 5-2 describes the basic Wi-Fi parameters.

Table 5-2 Basic Wi-Fi parameters

Parameter	Description
Enable WLAN	Indicates whether to enable the wireless network. The following parameters can be set only when the wireless network is enabled.
SSID	Indicates the name of the wireless network. It is used to differentiate different wireless networks. It consists of a maximum of 32 characters, without space or Tab character. A default SSID1, named WirelessNet is created after the creation of an ONT. The system can configure up to four SSIDs at a time and cannot assign IP addresses to Wi-Fi

Parameter	Description
	terminals by SSID.
Associated Device Number	Specifies the number of STAs. It ranges from 1 to 32.
Broadcast Ssid	<p>Indicates whether to enable or hide broadcast.</p> <ul style="list-style-type: none"> If the option box is selected, it indicates that the SSID broadcast function is enabled. The ONT periodically broadcasts the SSID, that is, the name of the wireless network. In this way, any STA can search for the wireless network. If the option box is not selected, it indicates that the SSID broadcast function is disabled. The SSID is hidden, and the STA cannot search for the wireless network. The SSID can be obtained only through a request.
WMM Enable	Indicates whether to enable the QoS of the wireless network. After the function is enabled, the video and voice QoS can be improved.
Authentication Mode	<p>Indicates the authentication mode for the STA to request access to the wireless network. The mode can be Open, Shared, WPA Pre-Shared Key, WPA2 Pre-Shared Key, WPA Enterprise, WPA2 Enterprise, or Wi-Fi Protected Setup.</p> <p>It is set to open by default, that is, the STA can access the network without authentication.</p>
Encryption Mode	<p>Indicates the encryption mode for the STA to request access to the wireless network. The encryption mode and encryption parameters vary with the authentication mode.</p> <ul style="list-style-type: none"> If the authentication mode is set to Open, the encryption mode can be set to None or WEP. If the authentication mode is set to Shared, the encryption is WEP. If the authentication mode is set to WPA Pre-Shared Key, WPA2 Pre-Shared Key, WPA Enterprise, or WPA2 Enterprise, the encryption mode can be set to AES, TKIP, or TKIP&AES. If the authentication mode is set to Wi-Fi Protected Setup, WPS Mode must be set to Pin or Push-button. <p>NOTE</p> <ul style="list-style-type: none"> Pin indicates the pin-based encryption. Push-button indicates the push-button-based encryption. <p>When WPS Mode is set to Push-button, press the WPS button on the ONT and press the WPS icon included with the STA within two minutes, or run the WPS setup program in the STA to install the WPS software.</p>

**NOTE**

- The security mode and encryption configured on a Wi-Fi terminal must be the same as those of an ONT. If the TKIP&AES, or AES encryption mode is not configured on the Wi-Fi terminal, the Wi-Fi terminal may have an old-version driver. If so, update the driver version.
- When two SSIDs are configured, if you modify the information of an SSID, the other SSID will re-choose a channel, causing the service to be interrupted for a few minutes.

5.5 Security

This topic describes how to configure the IP address filter, MAC address filter, DoS, and ONT access control through the Web page.

5.5.1 IP Filter Configuration

1. In the navigation tree on the left, choose **Security > IP Filter Configuration**. In the pane on the right, enable the IP address filter function. After selecting the filter mode, click **New**. Then, in the dialog box that is displayed, configure the rule for filtering IP addresses from the WAN interface to the LAN port, as shown in [Figure 5-13](#).

Figure 5-13 IP Filter Configuration

Security > IP Filter Configuration

On this page, you can configure the WAN-to-LAN filtering to prohibit certain IP addresses in the WAN from accessing the LAN.

Enable IP Filter: ☒

Filter Mode: BlackList

New Delete

Protocol	LAN-side IP Address	LAN-side Port	WAN-side IP Address	WAN-side Port

Configure

Protocol: TCP/UDP

LAN-side IP Address: 192.168.100.0 --- 192.168.100.99

LAN-side Port: ☒ ALL ☐ User-defined

WAN-side IP Address: ☒ ALL ☐ User-defined

WAN-side Port: ☒ ALL ☐ User-defined

Apply Cancel

2. Click **Apply** to apply the configuration.

The IP address filter function is a security mechanism configured on the residential gateway. It enables or disables all or partial ports in an Intranet IP address segment to communicate with all or partial ports in an Extranet IP address segment. The IP address filter configuration is used to limit communication between an Intranet device and an Extranet device.

[Table 5-3](#) describes the parameters related to the IP address filter.

Table 5-3 Parameters related to the IP address filter

Parameter	Description
IP address filter function	Indicates whether to enable the IP address filter function by clicking OPEN or CLOSE .
Filter Mode	Indicates the IP address filter rule of the blacklist or whitelist. <ul style="list-style-type: none"> Blacklist: indicates that the data meeting the rule in the filter rule list is not allowed to pass. Whitelist: indicates that the data meeting the rule in the filter rule list is allowed to pass. The filter mode is global config mode. Thus, the blacklist and whitelist mode cannot be used at the same time.
Protocol	Indicates the type of the protocol, which may be TCP/UDP, TCP, UDP, ICMP, or ALL.
LAN-side IP Address	Indicates the IP address on the LAN side.
LAN-side Port	Indicates the port ID on the LAN side. This parameter can be configured when Protocol is set to TCP/UDP , TCP or UDP .
WAN-side IP Address	Indicates the IP address on the WAN side.
WAN-side Port	Indicates the ID of the WAN side port. This parameter can be configured when Protocol is set to TCP/UDP , TCP or UDP .

5.5.2 MAC Filter Configuration

1. In the navigation tree on the left, choose **Security > MAC Filter Configuration**. In the pane on the right, after enabling MAC filter and selecting the filter mode, click **New**. On the dialog box that is displayed, configure the MAC filter rule for the PC to access the Internet, as shown in [Figure 5-14](#).

Figure 5-14 MAC Filter Configuration

Security > MAC Filter Configuration

On this page, you can configure the MAC filtering to prohibit certain PCs from accessing the Internet.

Enable MAC filter: ☒

Filter Mode: Blacklist

New Delete

Source MAC Address
00:15:17:2C:EF:97

Source MAC Address: 00:15:17:2C:EF:97 *(AA:BB:CC:DD:EE:FF)

Apply Cancel

2. Click **Apply** to apply the configuration.

The MAC address lists of PCs in the network are saved on the ONT. Configuring MAC filter rules enables the PCs that conform to the rules to access the Internet service or disables the PCs that do not conform to the rules to access the Internet service. A PC may have more than one IP addresses but a unique MAC address. Therefore, configuring MAC filter rules effectively controls the Internet service access rights of PCs in a LAN.

Table 5-4 describes the parameters related to the MAC filter.

Table 5-4 Parameters related to the MAC address filter

Parameter	Description
MAC address filter function	Indicates whether to enable the MAC address filter function by clicking OPEN or CLOSE .
Filter Mode	<p>Indicates the MAC address filter rule of the blacklist or whitelist.</p> <ul style="list-style-type: none">• Blacklist: indicates that the data meeting the rule in the filter rule list is not allowed to pass.• Whitelist: indicates that the data meeting the rule in the filter rule list is allowed to pass. <p>The filter mode is global config mode. Thus, the blacklist and whitelist mode cannot be used at the same time.</p>
Source MAC Address	Indicates the source MAC address in the MAC address filter rule.

5.5.3 URL Filter Configuration

1. Click the **Security** tab and then choose **URL Filter Configuration** from the navigation tree. In the pane on the right, after enabling URL filter and selecting the filter mode, click **New**. On the dialog box that is displayed, configure the URL filter rule for the PC to access the Internet, as shown in Figure 5-15.

Figure 5-15 URL Filter Configuration

Security > URL Filter Configuration

On this page, you can configure the parameters of URL filter. If enable smart URL filter, the data packets complying with the following URL rule are forbidden(or allowed) to pass the device when you access any site of the web server. otherwise only the data packets of your accessing site are forbidden(or allowed) to pass.

Enable URL Filter: ☒

Enable Smart URL Filter: ☒

Filter Mode: Blacklist

New Delete

URL Address
--

URL Address:

Apply Cancel

2. Click **Apply** to apply the configuration.

5.5.4 DoS Configuration

1. In the navigation tree on the left, choose **Security > DoS Configuration**. In the pane on the right, determine whether to enable the DoS attack-preventive configuration, as shown in [Figure 5-16](#).

Figure 5-16 DoS Configuration

Security > Dos Configuration

On this page, you can configure the DoS parameters, Denial of Service(DoS) is an attack action that decreases the availability of systems by preventing authorized users from accessing some special services.

Enable Prevent SYN Flooding Attack: ☐

Enable Prevent ICMP Echo Attack: ☐

Enable Prevent ICMP Redirect Attack: ☒

Enable Prevent Land Attack: ☐

Enable Prevent Smurf Attack: ☐

Enable Prevent Winnuke Attack: ☐

Apply Cancel

2. Click **Apply** to apply the configuration.

Denial of service (DoS) attack is a network-based attack that denies users from accessing the Internet. The DoS attack initiates a large number of network connections, making the server or the program running on the server break down or server resources exhaust or denying users to access the Internet service. As a result, the network service fails.

[Table 5-5](#) describes the parameters related to the DoS.

Table 5-5 Parameters related to the DoS

Parameter	Description
Prevent SYN Flooding Attack	<p>Indicates whether to enable the prevent SYN flooding attack.</p> <p>In the attack, several source hosts send SYN packets to a destination host. After receiving the SYN ACK packets from the destination host, the source hosts do not respond. In this case, the destination host establishes many connection queues for the source hosts and maintains these queues all the time because no ACK response is received. As a result, many resources are used and the destination host fails to provide normal services for normal connections.</p>
Prevent ICMP Echo Attack	<p>Indicates whether to enable the prevent ICMP echo attack.</p> <p>In the attack, many ICMP echo packets are sent to a destination host within a short time. As a result, the network is congested or the resources of the host are exhausted.</p>
Prevent ICMP Redirect Attack	<p>Indicates whether to enable the prevent ICMP redirect attack.</p> <p>In the attack, many ICMP redirect packets are sent to a destination host within a short time. As a result, the network is congested or the resources of the host are exhausted.</p>

5.6 Forward Rules

This topic describes how to configure the DMZ, port mapping, and port trigger through the Web page.

5.6.1 DMZ Configuration

1. In the navigation tree on the left, choose **Forward Rules > DMZ Configuration**. In the pane on the right, click **New**. In the dialog box that is displayed, set the parameters related to the DMZ, as shown in [Figure 5-17](#).

Figure 5-17 DMZ Configuration

Forward Rules > DMZ Configuration

On this page, you can configure the parameters of the DMZ device. The DMZ device provides services for unreliable external accesses. It is a buffer between a secure system and an insecure system. If the WAN port is not listed in the port mapping table, the application requests from the WAN connection are forwarded to the DMZ device.

NewDelete

	WAN Name	Enable DMZ	Host Address
Enable DMZ:		<input checked="" type="checkbox"/>	
WAN Name:	2_INTERNET_B_VID_1		
Host Address:	192.168.100.100		

ApplyCancel

2. Click **Apply** to apply the configuration.

The demilitarized zone (DMZ) is a technology that enables the ONT to forward all received packets through a specified internal server. The technology enables a computer in the LAN to be completely exposed to all users on the Internet or enables the mutual communication without restrictions between a host with a specified IP address and other users or other servers on the Internet. In this way, many applications can run on the host with the specified IP address. The host with the specified IP address receives all connections and files that can be identified.



NOTICE

If the LAN-side device does not provide website service or other network services, do not set the device to a DMZ host because all ports of a DMZ host are opened to the Internet.

Table 5-6 describes the parameters related to the DMZ.

Table 5-6 Parameters related to the DMZ

Parameter	Description
Interface Name	Indicates the name of the WAN interface. If the WAN interface is not in the port mapping table, the application requests from the WAN connection are directly forwarded to the host in the DMZ.
Host Address	Indicates the IP address of the DMZ host.
Enable DMZ	Indicates whether to enable the DMZ.

5.6.2 PortMapping Configuration

1. In the navigation tree on the left, choose **Forward Rules > Port Mapping Configuration**. In the pane on the right, click **New**. In the dialog box that is displayed, set the parameters related to port mapping, as shown in [Figure 5-18](#).

Figure 5-18 Port Mapping Configuration

Forward Rules > Port Mapping Configuration

On this page, you can set up virtual servers on the LAN network and allow these servers to be accessed from the Internet by setting port mapping parameters.
Attention: The well-known ports of voice can not be in the scope of the mapping port.

New Delete

WAN Name	Mapping Name	Protocol	External Port	Internal Port	Internal Host	Enable
Type:	<input checked="" type="radio"/> Custom	<input type="radio"/> Application	Select...			
WAN Name:	1_INTERNET_R_VI	Protocol:	TCP			
External Start Port:	123	External End Port:	124			
Internal Start Port:	200	Internal End Port:	201			
External Source Start Port:	145	External Source End Port:	146			
Internal Host:	192.168.100.100	External Source IP Address:	50.20.36.16			
Mapping Name:		Enable Port Mapping:	<input checked="" type="checkbox"/>			

Apply Cancel

2. Click **Apply** to apply the configuration.

Port mapping indicates that the Intranet server is allowed to be open to the Extranet (for example, the Intranet provides the Extranet with a WWW server or FTP server). Port mapping is to map the Intranet host IP address and port ID to Extranet IP address and corresponding port ID so that users from Extranets can access the Intranet server. With port mapping, the users cannot see the Intranet IP address and they see the Extranet IP address.

[Table 5-8](#) describes the parameters related to port mapping.

Table 5-7 Parameters related to port mapping

Parameter	Description
Interface	Indicates the name of the WAN interface where port mapping is enabled.
Protocol	Indicates the protocol type of port mapping packet, which may be TCP, UDP, or TCP/UDP.
External Start Port	Indicates the destination start port of the external data packet.
External End Port	Indicates the destination end port of the external data packet.
Internal Start Port	Indicates the internal destination start port of the port mapping packet.
Internal End Port	Indicates the internal destination end port of the port mapping

Parameter	Description
	packet.
External Source Start Port	Indicates the source start port of the external data packet.
External Source End Port	Indicates the source end port of the external data packet.
Internal Host	Indicates the IP address of the host to which the port is mapped.
External Source IP Address	Indicates the source IP address of the external data packet.
Mapping Name	Indicates the name of the port mapping rule.
Enable PortMapping	Indicates whether to enable port mapping.

5.6.3 PortTrigger Configuration

1. In the navigation tree on the left, choose **Forward Rules > Port Trigger Configuration**. In the pane on the right, click **New**. In the dialog box that is displayed, set the parameters related to the port trigger, as shown in [Figure 5-19](#).

Figure 5-19 Port Trigger Configuration

Forward Rules > Port Trigger Configuration

On this page, you can configure the range of the port that is used for the LAN-side applications to access the Internet and enable the port automatically.

New Delete

	WAN Name	Status	Trigger Port	Open Port	Trigger Protocol	Open Protocol
Enable Port Trigger:		<input checked="" type="checkbox"/>				
WAN Name:	1_INTERNET_R_VID_150					
Trigger Protocol:	UDP					
Open Protocol:	UDP					
Trigger Start Port:	200					
Trigger End Port:	201					
Open Start Port:	145					
Open End Port:	146					

Apply Cancel

2. Click **Apply** to apply the configuration.

The port trigger indicates that a specific Extranet port is automatically enabled when a corresponding Intranet port sends a packet and the packet is mapped to the Intranet port on the host. A specific mapping packet is sent from the ONT through the Intranet so that specific packets of the Extranet can be mapped to the corresponding host. A specified port on the gateway firewall is open to some applications for remote access. The port trigger can dynamically enable the open port of the firewall.

Table 5-8 describes the parameters related to the port trigger.

Table 5-8 Parameters related to the port trigger

Parameter	Description
Interface	Indicates the name of the WAN interface where the port trigger is enabled.
Trigger Protocol	Indicates the protocol type of the port trigger packet, which may be TCP, UDP, or TCP/UDP.
Open Protocol	Indicates the protocol type of the open data packet.
Trigger Start Port	Indicates the destination start port of the port trigger packet.
Trigger End Port	Indicates the destination end port of the port trigger packet.
Open Start Port	Indicates the destination start port of the open packet.
Open End Port	Indicates the destination end port of the open packet.
Enable	Indicates whether to enable the port trigger.

5.7 Network Applications

This topic describes how to configure the USB, ALG, UPnP, and ARP through the Web page.

5.7.1 USB

1. In the navigation tree on the left, choose **Network Applications > USB**. In the pane on the right, set the parameters related to FTP downloading to share the FTP file of the ONT, as shown in Figure 5-20.

Figure 5-20 USB

Network Application > USB Application

FTP Client Configuration

You can download the file from FTP server to the USB mass storage device by config FTP client.

FTP URL:

ftp://192.168.100.3/*.*

Port Number:

21

User Name:

123

Password:

...

Device:

No USB Device

Local Path:

Download

User Name	Password	Port Number	Download URL	Local Path	State
--	--	--	--	--	--

FTP Server Configuration

You can share data of USB mass storage device in LAN by config FTP Server.

Enable FTP Server:

☒

User Name:

root

Password:

.....

Device:

No USB Device

Root Directory Path:

ApplyCancel

2. Click **Download** to download files from the FTP server to the USB storage device.

Table 5-9 describes the parameters related to the USB.

Table 5-9 Parameters related to the USB

Parameter	Description
Download URL	Indicates the path of the file downloaded through FTP.
Port Number	Indicates the FTP port number. It is set to 21 by default. Generally, the setting is not required.
User Name	Indicates the user name for connecting to the FTP server. If the FTP server supports anonymous login, the setting is not required.
Password	Indicates the password for connecting to the FTP server. If the FTP server supports anonymous login, the setting is not required.
Device	Indicates the drive of the external USB device for saving the file downloaded through FTP. When the USB storage device is connected to the USB port, the drop-down list is available.
Local Path	Indicates the path for saving the FTP-downloaded file to the external USB device. If the path is not entered, the path

Parameter	Description
	specified in Download URL is used by default.

5.7.2 ALG Configuration

1. In the navigation tree on the left, choose **Network Applications > ALG Configuration**. In the pane on the right, determine whether to enable the FTP or TFTP, as shown in [Figure 5-21](#).

Figure 5-21 ALG Configuration

2. Click **Apply** to apply the configuration.

When the NAT function is enabled, the application level gateway (ALG) function needs to be enabled to ensure that some application software and hardware can be normally used.

5.7.3 UPnP Configuration

1. In the navigation tree on the left, choose **Network Applications > UPnP Configuration**. In the pane on the right, determine whether to enable the UPnP, as shown in [Figure 5-22](#).

Figure 5-22 UPnP Configuration

2. Click **Apply** to apply the configuration.

Universal Plug and Play (UPnP) is the name of a group of protocols. The UPnP supports zero configuration networking and automatic discovery of different network devices. If the UPnP is enabled, the UPnP-enabled device can be dynamically connected to the network to obtain the IP address, obtain the transfer performance, discover other devices, and learn the performance of the other devices. The UPnP-enabled device can be automatically disconnected from the network, without affecting the device or other devices.

When the UPnP is enabled, the LAN-side PC automatically finds the ONT, which is considered as a peripheral device of the PC and is plug-and-play. After running application software on the PC, port mapping entries are automatically generated on the ONT through the UPnP protocol, thus improving the running speed.

5.7.4 ARP Configuration

1. In the navigation tree on the left, choose **Network Applications > ARP Configuration**. In the pane on the right, click **New**. In the dialog box that is displayed, set the resolution rule between a MAC address and an IP address, as shown in [Figure 5-23](#).

Figure 5-23 ARP Configuration

	IP Address	MAC Address
IP Address:	192.168.100.100 *	
MAC Address:		00:15:17:2C:EF:97 *

2. Click **Apply** to apply the configuration.

Static ARP means to manually add an ARP entry on an ONT. A static ARP never ages and can only be deleted manually. If the mapping between the IP address and MAC address of the peer device is available, configuring a static ARP entry benefits a lot. For example, the dynamic ARP entry learning is omitted during device communication and the static ARP entry prevents a device from learning an incorrect ARP entry in the case of malicious attacks.

5.7.5 DDNS Configuration

1. Click the **Network Application** tab and then choose **DDNS Configuration** from the navigation tree. In the right pane, configure DDNS parameters, including **Service Provider**, **Host Name**, **Service Port**, **Domain Name**, **Username**, and **Password**, as shown in [Figure 5-24](#).

Figure 5-24 DDNS configuration

Network Application > DDNS Configuration

On this page, you can configure the DDNS parameters, including the service provider, the username and password, also the domain name you want to update.

New Delete

	WAN Name	Status	Service Provider	Domain Name
Enable DDNS:	<input checked="" type="checkbox"/>			
WAN Name:	1_INTERNET_R_VID_1			
Service Provider:	dyndns-static			
Host Name:	members.dyndns.org			
Service Port:	80			
Domain Name:	www.abc123.com			
Username:	user			
Password:	••••			

Apply Cancel

2. Click **Apply** to apply the configuration.

Dynamic domain name service (DDNS) associates a static domain name with the dynamic IP address of its host.

Assume that server A provides HTTP or FTP service and it is connected to the Internet using routers. If server A obtains an IP address through DHCP, or server A is connected to the Internet through PPPoE, PPTP, or L2TP, the IP address is a dynamic IP address. That is, its IP address may change each time when server A initializes its connection to the Internet.

The mapping between the domain name and IP address provided by the domain name service (DNS) server is static, and the mapping does not update when the IP address changes. Therefore, when the IP address of server A changes, users on the Internet cannot access server A with domain names.

With DDNS, which associates a static domain name with the dynamic IP address of its host, users on the Internet can access the server only with domain names.

5.7.6 IGMP Configuration

1. Click the **Network Application** tab and then choose **IGMP Configuration** from the navigation tree. In the right pane, configure the IGMP parameters, as shown in [Figure 5-25](#).

Figure 5-25 IGMP configuration

Network Application > IGMP Configuration	
On this page, you can set the IGMP parameters; You can enable the IGMP for the WAN interface by choosing HomeGateway as the IGMP work mode. You can configure the parameters such as robustness, general query interval, general response time, special query number, special query interval and special response time only when IGMP work mode is HomeGateway and IGMP proxy are enabled.	
IGMP Enable:	Enable
IGMP Work Mode:	Proxy
Robustness:	2 (1~10 default value: 2)
General query interval:	125 (30~5000s default value: 125s)
General query response time:	100 (1~255 unit: 0.1s default value: 100)
Specific query number:	2 (1~10 default value: 2)
Specific query interval:	10 (1~5000 unit: 0.1s default value: 10)
Specific query response time:	10 (1~255 unit: 0.1s default value: 10)
Apply Cancel	

2. Click **Apply** to apply the configuration.

The IGMP function of WAN ports can be enabled only when IGMP works in the gateway mode. Only when IGMP proxy is enabled in the gateway mode, parameters such as **Robustness**, **General query interval**, **General query response time**, **Specific query number**, **Specific query interval**, and **Specific query response time**.

5.7.7 QoS Configuration

1. Click the **Network Application** tab and then choose **QoS Configuration** from the navigation tree. In the right pane, enable/disable QoS and select a QoS mode, as shown in [Figure 5-26](#).

Figure 5-26 QoS configuration

Network Application > QoS Configuration	
On this page, you can set the QoS parameters. You can enable or disable QoS service and select a mode for QoS.	
Enable QoS:	<input checked="" type="checkbox"/>
QoS Mode:	INTERNET,TR069
Apply Cancel	

1. Click **Apply** to apply the configuration.

5.7.8 DNS Configuration

1. Click the **Network Application** tab and then choose **DNS Configuration** from the navigation tree. In the right pane, configure DNS parameters, as shown in [Figure 4-27](#)

Figure 5-27 DNS Configuration

	Domain Name	DNS Server
Domain Name:	www.huawei.com	DNS Server:
		10.172.10.10

2. Click **Apply** to apply the configuration.

5.8 System Tools

This topic describes how to use the system tools on the Web page, including using the tools to restart the device, restore the default configuration, and conduct the test.

5.8.1 Reboot

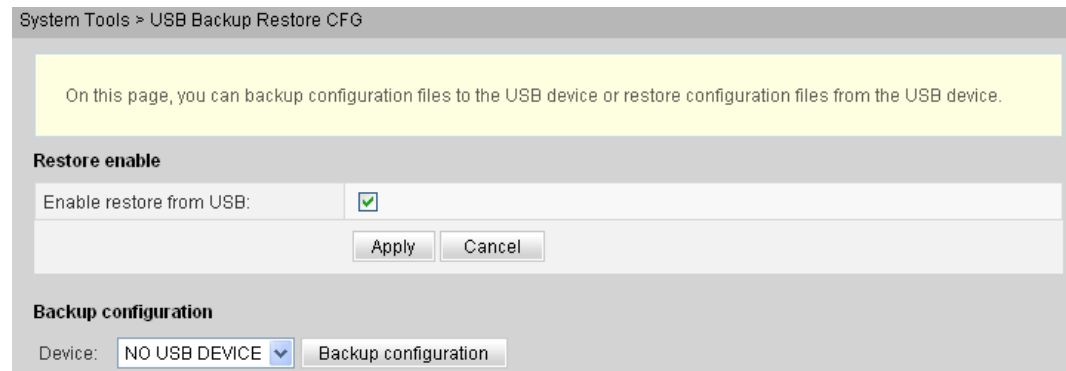
In the navigation tree on the left, choose **System Tools > Reboot**. In the pane on the right, click **Reboot** to restart the device, as shown in [Figure 5-28](#).

Figure 5-28 Reboot

5.8.2 Configuration File

Click the **System Tools** tab and then choose **Configuration File** from the navigation tree. In the pane on the right, the button as required, as shown in [Figure 5-29](#).

Figure 5-29 USB Backup Restore CFG



- Select **Enable restore from USB** to configure whether the system supports fast recovery of the backed up configured file from the USB storage device.
- Click **Backup configuration** to back up the configuration file to the specified USB storage device.



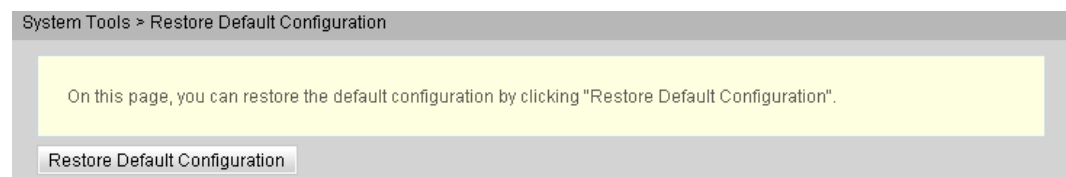
NOTICE

After the configuration file in the USB storage device is successfully uploaded, the device is restarted and then the new configuration data takes effect.

5.8.3 Restore Default Configuration

In the navigation tree on the left, choose **System Tools > Restore Default Configuration**. In the pane on the right, click **Restore Default Configuration** to restore the factory defaults, as shown in [Figure 5-30](#).

Figure 5-30 Restore Default Configuration



NOTICE

Exercise caution when you perform this operation because it restores factory defaults.

5.8.4 Maintenance

In the navigation tree on the left, choose **System Tools > Maintenance**. In the pane on the right, enter the destination IP address for the ping and tracert test in the **Target** text box, and then click **Start**, as shown in [Figure 5-31](#).

Figure 5-31 Ping test

System Tools > Maintenance

On this page, you can check the connectivity to the LAN or the Internet by performing a Ping Test.

Ping Test

Target:

WAN Name:

Tracert Test

You can check the connectivity to the LAN or the Internet by performing a Tracert Test.

WAN Name:

Target:

Maintenance

To end maintenance, please click the "Maintenance End" button.

- If the ping test is successful, **The result** is displayed as **PASS**, that is, the ONT can interwork with the device with the destination IP address.
1. If the ping test fails, **The result** is displayed as **FAIL**, that is, the ONT cannot interwork with the device with the destination IP address.

5.8.5 Voice Remote Mirroring

1. In the navigation tree on the left, choose **System Tools > Voice Remote Mirroring**. Configure the capture packets in or out of CPU, and then click Start, as shown in [Figure 5-32](#).

Figure 5-32 Voice Remote Mirroring Configuration



NOTE

- The Remote Mirror Capture is to mirror the files on the user side (no time limit).
1. The Mirror Capture is to mirror the file into the flash of ONT (can not be stored for long periods).

5.8.6 Log

In the navigation tree on the left, choose **System Tools > Log**. In the pane on the right, click **Download log File**. In the dialog box that is displayed, click **Save**, specify the path of saving the log file, and save the file to the local disk, as shown in [Figure 5-33](#).

Figure 5-33 Log

5.8.7 ONT Authentication

1. In the navigation tree on the left, choose **System Tools > ONT Authentication**. In the pane on the right, you can view or change the authentication mode for the registration of the ONT on the OLT, as shown in [Figure 5-34](#).

Figure 5-34 ONT Authentication

System Tools > ONT Authentication

On this page, you can change the parameters for authentication on the OLT. Reset the ONT after changing the parameters.

Authentication Mode:	<input type="radio"/> LOID	<input checked="" type="radio"/> Password
Password Mode:	ASCII String	
Password:	12345678	(The password must be between 1-10 characters)
SN:	48575443765E8510	*(The SN must be a 16-digit hexadecimal number)
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

- Click **Apply** to apply the configuration.



NOTE

The user can modify the ONT SN by using the phone on condition that the ONT has never been online. Otherwise, the ONT cannot be modified. The modification is performed as follows:

Connect the phone to the POTS port on an ONT, dial "***SN**SN#" (SN indicates ASCII codes), and then restart the ONT.

5.8.8 Advanced Power Management

- In the navigation tree on the left, choose **System Tools > Advanced Power Management**. In the pane on the right, you can start the ONT energy conservation mode and set the power saving mode, as shown in [Figure 5-35](#).

Figure 5-35 Advanced Power Management

System Tools > Advanced Power Management

On this page, you can set the power management mode of the ONT.

Enable power mode configuration

Enable: ☒

Check the box under "Enable" to continue to use the service while the system is in battery (backup) mode.

Service Type	Enable
USB:	<input checked="" type="checkbox"/>
LAN:	<input checked="" type="checkbox"/>
WLAN:	<input checked="" type="checkbox"/>
VOICE:	<input checked="" type="checkbox"/>
CATV:	<input checked="" type="checkbox"/>
Remote Management:	<input checked="" type="checkbox"/>

- Click **Apply** to apply the configuration.

5.8.9 Modify Login Password

1. Click the **System Tools** tab and then choose **Modify Login Password** from the navigation tree. In the right pane, change the password of the **root** user, as shown in [Figure 5-36](#).

Figure 5-36 Modify Login Password

System Tools > Modify Login Password

On this page, you can change the password of the ordinary user to ensure security and make it easy to remember.

Username:	root
New Password:	<input type="password"/> (Password length must be from 9 to 30 characters long, and it must include one special character at least.)
Confirm Password:	<input type="password"/>

2. Click **Apply** to apply the configuration.

6 FAQs

THE LOS INDICATOR BLINKS.

- If the LOS indicator blinks once two seconds, check whether the pigtail fiber is properly connected and the connector is clean.
- If the GPON terminal blinks twice a second, contact the service provider for help.

THE PON INDICATOR IS OFF.

- Check whether the OPTICAL port and optical fiber is properly connected.
- The GPON terminal fails to register with the upper-layer device. Contact the service provider for help.

THE PHONE DOES NOT RING UPON AN INCOMING CALL BUT COMMUNICATION IS IN NORMAL STATE WHEN THE PHONE IS IN OFF-HOOK STATE.

- The GPON terminal provides a maximum of 60 V AC ringing current voltage. Check whether the ringing current voltage of the phone is higher than 60 V AC. If it is higher than 60 V AC, replace it with another phone.

HOW TO RESET THE GPON TERMINAL?

- Press RESET by using a needle-type object.

HOW CAN I RESTORE FACTORY DEFAULTS?

- Press RESET by using a needle-type object for longer than 10s to restore factory defaults and reset the GPON terminal. If the indicator is off and then is lit, the system restarts successfully.

7 Acronyms and Abbreviations

ALG	Application Level Gateway
BRAS	Broadband Remote Access Server
CATV	Community Antenna Television
DBA	Dynamic Bandwidth Assignment
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name Server
DoS	Denial of Service
FTP	File Transfer Protocol
FTTH	Fiber To The Home
GPON	Gigabit-capable Passive Optical Network
HTTP	Hyper Text Transport Protocol
IGMP	Internet Group Management Protocol
ISP	Internet Service Provider
LAN	Local Area Network
MAC	Media Access Control
NAPT	Network Address and Port Translation
NAT	Network Address Translation
NMS	Network Management System
OLT	Optical Line Terminal
OMCI	Optical Network Termination Management and Control Interface
PON	Passive Optical Network
PPPoE	Point to Point Protocol over Ethernet
PSTN	Public Switched Telephone Network
SIP	Session Initiation Protocol
SOHO	Small Office and Home Office
SSID	Service Set Identifier

STB	Set Top Box
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
UDP	User Datagram Protocol
UPnP	Universal Plug and Play
URL	Uniform Resource Locator
VLAN	Virtual Local Area Network
VoIP	Voice over IP
WLAN	Wireless Local Area Network
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
WPS	Wi-Fi Protected Setup